State of Connecticut

Security Domain
Technical Architecture

January 4, 2001
Version 1.0

History of Changes

11/29/2000	Added an appendix with a copy of the State's Network Security Policy

Table of Contents

List of Tables

Mission Statement

The State of Connecticut's information and information systems are valuable assets that must be protected. The state must maintain compliance with legal requirements for confidentiality and integrity while enabling public access to appropriate information. Security Architecture identifies criteria and techniques associated with protecting and providing access to the state's information resources. It facilitates identification, authentication, authorization, administration and audit. The state's technological resources must be available to users across the enterprise regardless of location or platform. Therefore, the state must implement security in such a manner that its information infrastructure is protected and accessible while, at the same time, its functionality is unimpeded and its business services are readily available.

Introduction and Background

We are developing closer electronic partnerships with businesses outside of state government, some employees are mobile users, some employees are working from their homes, and state services are being brought closer to the citizen electronically. The purpose of security is to protect and secure the state's information resources in order to provide an environment in which the state's business can be safely transacted. A directory is a natural place to centralize management of security. It is the vault that contains the most trusted and critical components of an enterprise security strategy. This will require authorization and authentication services and a common enterprise repository of digital certificates that secures and supports E-commerce applications. Security services apply technologies to perform the functions needed to protect assets. Historically, such services have consisted of door locks, vaults, guards, sign-in/sign-out logs, etc. As the state performs more business functions electronically, it must transition to security services designed to protect the electronic environment. For example, the use of face-to-face identification must be superceded by an equivalent electronic method that does not require the physical presence of the person.

Traditional Business Versions	**Electronic Business Versions**
Handwritten signatures	Digital signatures
Visual identification of individuals and business partners	Biometrics, smart cards, token cards, Public Key Certificates
Notary services	Digital time stamping and digital signatures
Visual inspection of documents to detect modifications	Integrity and cryptography services

A database that provides methods to inventory, administer, and access resources in the network is a directory service. Resources may include users, groups of users, applications, data, printers, servers, and other physical devices throughout the network. If a directory service is properly planned and executed, it can provide a central point for authentication (log-in) and a survey of all available resources on the network. Furthermore, this brings about authorization, also known as access control, which determines the rights that are associated to a particular resource and enforces them. Directory services offer network users, administrators, and applications transparent access to all network resources and easy navigation of the network. As the electronic age transitions from closed, proprietary systems to more open, distributed systems, additional

security services will be needed to provide protection in a dynamic and less controllable environment. For example, the use of simple electronic passwords within a local network might be supplemented by biometrics-based identification methods when used across the Internet. Therefore, the state must create a security architecture that will provide the strategies and framework necessary to protect its information infrastructure while it transacts business in a changing electronic world. In order to protect its resources, the state must first assess the types of threats that it will encounter relative to its information infrastructure. It must understand the forms of threats that are possible in the electronic technology environment and it must determine what impact any particular threat will have on the state's business. Once the state understands how its information infrastructure could be threatened, it must develop a security architecture to defend itself. The security architecture must identify the basic services needed to address security in both the current electronic environment and in future, anticipated electronic environments. It must also recognize the various types of threats and protect itself from them. The architecture must address the various technologies available to implement the desired services.

Component Topics

The required security services to protect the state's information infrastructure will be discussed in this document as component topics. They include:

- Privacy and Confidentiality – The policy governing the state's responsibility of how it collects and manages data.
- Access Control – The process of protecting the state's internal networks by deployment of firewalls and proxies.
- Administration Tools – Hardware and software systems which enable analysis and verification of the security infrastructure.
- Authentication – The means of establishing and verifying the identity of the user.
- Cryptography – The technology used to protect the confidentiality of information.

Component Topic 1: Privacy and Confidentiality

A **privacy policy** should be published on every government web site, even if the site does not create records of the information collected. A privacy statement should explain how information is managed. Because state agency web sites have many different purposes, the privacy policies found on these sites should also be diverse and specific to the visited site. A "one size fits all" approach to developing a privacy policy will not effectively or accurately reflect the information gathered by individual agencies or how they process and store this information. Specific web-based forms that require personal information should post a privacy policy, or a link to the policy, at the top of the page/form. This policy should indicate how the information will be used and under what conditions the information may be shared or released to another party. The form may include a provision for the individual to opt-out of sharing the information with another party or a warning that the information may be a public record and subject to an FOI request. Web pages designed for children must comply with all applicable federal (i.e., Children's Online Privacy Protection Act) and state laws intended to protect minors.

Introductory Language

The policy should identify the agency and should include a short overview of privacy practices and how they apply to the site.

Example:

The (agency name) maintains the web site as a public service. The following is the privacy policy for this site (use www.state.<domain name>.us):

Information Collected and Stored Automatically

In the course of operating a web site, certain information may be collected automatically in logs or by cookies. Some agencies may be able to collect a great deal of information, but according to policy, choose to collect only limited information. In some instances, agencies may have the technical ability to collect information and later take additional steps to identify people, such as looking up static Internet Protocol addresses that can be linked to specific individuals. Regardless of an agency's decision to collect this type of information or take further steps to gather more information, the privacy statement must clearly denote the policy. It is imperative to ensure these policies are consistent with the State's.

Freedom of Information laws.

Example: We do not use cookies to collect information. Note: A cookie file contains unique information a web site can use to track such things as passwords, lists of pages you've visited, and the date when you last looked at a specific page. Cookies often are used to identify your session at a particular web site. A cookie is often used in commercial sites to identify the items selected for a specific shopping cart application. (Note: If the site uses cookies, the policy should identify what information is collected and how that information is used and protected. The main home page and privacy policy page should not require the visitor to accept, or set, a cookie.) For site management functions, information is collected for analysis and statistical purposes. This information is not reported or used in any manner that would reveal personally identifiable information. This information will not be released to any outside parties unless legally required to do so in connection with law enforcement investigations or other legal proceedings. We use Log analysis tools to create summary statistics, which are used for purposes such as assessing what information is of most interest, determining technical design specifications, and identifying system performance or problem areas.

Component Topic 2: Access Control

Firewall technology is rapidly evolving. There are two basic types, packet filtering and application gateways (proxy servers). The network architecture and location of firewalls relative to internal networks is an important consideration in securing internal networks.

Technology 1: Firewalls

Firewalls are a common term for physical devices, software and network architectures designed to block or filter access between a private network and a public network such as the Internet. They can also be used to provide access control between separate internal networks. Firewalls enforce the enterprise's security policy at determined perimeters, e.g., access point to the public Internet. To be effective, each must provide the single point of access to and from an un-trusted network. Packet-filtering firewalls filter access at the packet level. By examining the contents of packets, they permit or deny access based on a defined access control policy. Packet filtering firewalls operate below the application and typically do not have access to information particular to an application. The network architecture used in deploying firewalls can add additional protection. By placing a sub-network between the internal network behind the firewall and the external public Internet, multiple security breaches would be required to penetrate the internal network. This additional sub-network is referred to as a 'demilitarized zone' (DMZ). Multiple DMZs can be employed to protect sub-networks within the enterprise.

Technology 2: Proxy

Application level firewalls or proxy servers protect internal networks by not permitting direct access from the internal network to un-trusted networks such as the public Internet. Internal users connect to the 'proxy' which then acts on their behalf, completing the connection to the requested external service. Proxy firewalls are specific to the applications they proxy. For example, a proxy for Web or FTP is installed to support those applications. Not all applications can be proxied. For those that can't be proxied, proxy-like gateways shuttle data between internal and external networks. They maintain the characteristic of preventing direct connections between the internal and external networks.

Component Topic 3: Administration Tools.

The security architecture must provide the capability to track and monitor successful and unsuccessful interactions with the information infrastructure. Accountability for interactions must be tied to specific users. The architecture should be able to audit all significant security events including authentication, accessing of services and security administration.

Assessment services are based on a methodology of deterministic, comprehensive, and practical analysis of networks and systems, from policy and architecture to details of system configuration and use. The assessment is designed to ensure that the system operates with sufficient security to meet its requirements without unacceptable risks of compromise to information assets or services.

An essential part of the process is the study of business, design, and implementation issues that could allow the system to fail to meet security and functional requirements, either inadvertently or through the inducement of an outside agency. Business issues of interest include system objectives, assets and threats, business relationships and contracts, system boundaries and privacy expectations. Design issues include network and security architecture, physical security, application functions, data retention/destruction, and use of cryptography, logging, and usability.

Technical analysis includes administrative procedures, cryptographic procedures, inspection of hosts and network devices, physical site inspection, external network scans, and design or code review of critical applications.

Examples of tools to facilitate this analysis are Protocol Analyzers, Scanning Tools, Password Integrity programs, and operating system vulnerability tests.

Technology 1: Intrusion Detection Systems.

Intrusion Detection System (IDS) technology is an important component of a comprehensive enterprise security strategy. IDS products alert security administrators of suspicious activity that may be occurring on their systems and networks in real time. It has long been a subject of theoretical research, but is now gaining mainstream popularity.

Technology 2: Protocol Analysis Software.

Protocol Analysis Software is a powerful network visibility tool that enables the security administrator to monitor network traffic in real time, collect detailed utilization and error statistics for individual stations, and save historical utilization and error information for baseline analysis. Additionally, these systems can generate visible and audible real-time alarms, and notify security administrators when troubles are detected. Network traffic can be captured for detailed packet analysis, and probes can be conducted to simulate traffic, measure response times, count hops, and troubleshoot problems.

Technology 3: Vulnerability, Scanning, and Penetration Testing Tools.

Vulnerability Assessment products complement IDS very well. They help determine the overall security posture of a system or network, and allow security administrators to identify and fix vulnerabilities before an attacker can exploit them. Some products are designed to simulate an actual attack, using known hacker methodology and attack signatures.

Technology 4: Email Content Filtering and Virus Scanning Systems.

An Email content filtering and virus scanning system can allow the security administrator to easily manage, filter and if necessary block unauthorized company communications made

through e-mail, newsgroups and FTP sites. This component is more than a simple filtering product since it can determine the *content and context* of e-mails, FTP downloads, newsgroup postings and "spam" that's going into, out of, or through the state's network. This approach goes beyond simple keyword string matching to reporting results that are more accurate. This enables the security administrator to properly enforce the state's Acceptable Usage Policy for corporate electronic communications to

- limit legal liability from offensive messages,
- protect sensitive and confidential information from leaks via e-mail,
- reduce network congestion caused by e-mail attachments and "spam", and
- ensure that file attachments are scanned for virus or attack signatures prior to their delivery to recipients.

Technology 5: Centralized LAN/WAN Management Console

Since this is in the standards section, shouldn't there be some discussion here first?

Component Topic 4: Authentication

Authentication is the act of verifying the identity of a user or process. Authentication answers the question: "Are you who you say you are?" The most common method used to authenticate a user is a password. A password is a secret series of characters and numbers associated with an individual user id by the owner/user. A sign-on process to authenticate the user accepts a password and a user-id. The sign-on process matches the password given, with a stored password for that user. If they match, the system has verified the user's identity. Passwords are inexpensive and widely integrated into today's systems. Passwords have various weaknesses. User passwords are often poorly chosen, lack adequate administration, and present a danger of passwords being intercepted and read over unsecured communication links.

Electronic business transactions have stricter requirements on uniquely identifying and authenticating the sender or recipient of electronic information. These can be satisfied with a 'digital signature,' which is the equivalent of a handwritten signature. Authentication techniques such as Public Key Certificates have been developed to address the strict authentication requirements of electronic business processes. The technology components used in authentication are based on existing and emerging standards. Implementation differences, even where standards are used, can raise barriers to enterprise-wide solutions. For an enterprise-wide security infrastructure to succeed, the technologies must use open protocols and standards. Complete solutions do not exist, but the basic building blocks are available.

Technology 0: Mainframe

Since this is in the standards section, shouldn't there be some discussion here first?

Technology 1: Remote Access

Remote Access is defined as a user outside the normal boundaries of the state's network connected through external means, such as a dial-up or Internet connection. This mode of access is increasing due to the mobility of employees, and the increasing requirement of providing access to state systems for vendors and business partners. There must be assurance that these methods of access are secure and cannot be compromised.

Technology 2: Proprietary Token-based Authentication

Tokens are physical cards similar to credit cards that work in conjunction with a user id to identify a user to the system. They combine something a person knows, such as a password or

PIN, with something they possess, a token card. Token cards commonly generate either dynamic passwords or a response in a challenge-response communication between the user and the system. These tokens work together with server based systems to match a token holder to a user profile, normally referred to as Authentication Servers.

Technology 3: Biometrics

A biometrics is a unique, measurable physical or behavioral characteristic of a human being for automatically recognizing or verifying identity. Biometrics characteristics can include fingerprints, iris data, hand and face geometry, signature, voice and DNA. Each of these methods has different degrees of accuracy, cost, social acceptability and intrusiveness. An extreme example of an intrusive technique would be a DNA sample. Voice identification would be an example of a non-intrusive and socially acceptable technique.

All biometrics products operate in a similar way. First, a system captures a sample of the biometrics characteristic during an enrollment process. Unique features are then extracted and converted by the system into a mathematical code. This code is then stored as the biometrics template for that person. The template may be stored in the biometrics system itself, or in any other form of memory storage, such as a database, a smart card or a barcode. When a user needs to be identified, a real-time sample is taken and matched against stored templates. If the match is within pre-defined tolerances, the individual's identity is established.

There is no perfect biometrics technique for all uses. Some biometrics techniques may be more suitable for particular situations. Factors can include the desired security level and the number of users. For instance, identifying a user for access to the state's systems matches that user to their known biometrics template (one-to-one match). This is easier than identifying a welfare applicant from the larger set of existing recipients to reduce duplication of benefits (one-to-many match). Identification of a remote user may require a biometrics that can be captured remotely, for example, voice identification using a telephone.

Biometrics systems are not 100% accurate. Accuracy in biometrics is measured by false acceptances versus false rejects. False acceptances are when an unauthorized user is allowed access. A false reject is when an authorized user is denied access. Thresholds can be adjusted to reduce one type of error at the expense of increasing the other. The choice of threshold depends on the level of security required, the acceptability of the type of error, and user acceptability.

The accuracy of biometrics can also be improved by combining two techniques such as fingerprint identification and face recognition. An intersection of the matches from two biometrics techniques typically results in an acceptable identification. Examples of types of biometrics are Fingerprint, Hand Geometry, Iris, Face Geometry, Voice, and Signature.

Component Topic 5: Cryptography

Documents, communications and data travel inside and outside the enterprise in electronic form. Electronic information is easy to read, modify or replace without detection. However, in many situations, the confidentiality of the information in transit must be maintained, e.g., taxpayer data, credit card and bank account numbers, and child abuse cases.

Information transported across the state's TCP/IP networks and across the public Internet is passed in clear text. Malicious individuals can intercept, view and modify this information using easily obtained tools. As described in the authentication section above, cryptography is a means to scramble information such that only authorized entities (people or processes) have access to

the information. A combination of public key cryptography and secret key cryptography can be used to implement authenticated and protected communication for secure access control. Most bulk encryption of information involves the use of secret key cryptography.

Technology 1: Public Key / Private Key technology

Authentication which requires the unique identification of a user is often based on Public / Private Key cryptography. This form of cryptography uses two *related* keys. Information encrypted with one key can *only* be decrypted with the other key. The 'Public' Key is made openly available in a repository to anyone who wants to communicate with the user in a secure manner. The 'Private' Key is kept *only* by the owner and is *never* divulged. Since only the owner has the private key, its use is considered sufficient to uniquely authenticate the owner. A digital signature is an example of a private key being used to verify that the sender (originator of the information) is really who they say they are. An example illustrates how a taxpayer by using their private key authenticates themselves to a tax department. The tax department recovers the taxpayer's information by using the taxpayer's public key. Since only the taxpayer's public key can recover what was encrypted with the taxpayer's private key, the tax department is assured it came from this particular taxpayer. A user's public key is distributed using an electronic document called a Public Key Certificate. This certificate contains the user's name, public key, an expiration date and other information. It is considered reliable when a trusted authority digitally signs it. Trusted authorities that issue certificates are known as Certificate Authorities.

Technology 2: Digital Signature

Digital signatures are the equivalent of a handwritten signature in that they tie an individual to a document. The first step in digitally signing an electronic document is to generate a message digest of the document. The signer encrypts this message digest using the signer's unique private key. The document and encrypted message digest are sent to one or more recipients. Verifying a digital signature is the reverse process. The recipient generates a message digest from the document. By using the signer's public key, the recipient can recover the original message digest from the encrypted one. This proves it must have come from the signer since only they have the private key. If the recovered and the generated message digests are equal, the document has not been modified and the sender cannot deny their digital signature. The digital signature, therefore, provides non-repudiation, which means that the sender cannot falsely deny having sent the message.

Technology 3: Secret Key Cryptography

Secret key technology is a form of cryptography where encryption and decryption use the same key, a 'secret' key. Pairs of users or processes share the same secret key. Data encrypted with a secret key is decrypted using the same secret key. Secret key technology is used to do most encryption because it is much faster than other techniques. Examples of commonly used secret key algorithms include DES, 3-DES, RC2, RC4, IDEA and CAST.

Technology 4: Security Protocols

Protocols are well-defined message formats used for communicating in networked systems. Security protocols provide security functions. The lack of a of set widely inter-operable stable standards raises barriers to enterprise- wide solutions. When considering products, it is useful to check present and future planned compliance to standards. Important security protocols are described below:

Secure Sockets Layer – SSL is a widely used means for securely communicating between a Web browser and Web server. SSL creates an encrypted link between a client and server that

need to communicate securely. Both client and server authentication is possible. SSL can also be used with other applications such as ftp, telnet, *etc*.

Simple Key Management for Internet Protocols – SKIP is a "secret key exchange protocol" that operates below the IP layer in a TCP/IP communications protocol. This method can be used to provide transparent security between entities.

Security Multi-parts for MIME – S/MIME is an application security protocol. It is implemented for email but it has wider implications for store-and-forward messaging.

Internet Protocol security extensions – IPSec is a security protocol defined for IP networks which operates at the network layer in TCP/IP communications protocol. IPSec adds header extensions to the IP communications protocol, designed to provide end-to-end security for packets traveling over the Internet. IPSec defines two forms: sender authentication and integrity, but not confidentiality, using an Authenticating Header (AH), and sender authentication, integrity and confidentiality using an Encapsulating Payload (ESP).

Internet Key Exchange – IKE provides secure management and exchange of cryptographic keys between distant devices. It is the standard key exchange mechanism for IPSec.

Technology 5: Virtual Private Networks (VPNs)

Virtual private networks are ways of connecting two networks or trading partners that must communicate over insecure networks such as the public Internet. A VPN establishes a secure link by using a version of the IPSec security protocol. These links are typically implemented between firewalls. VPNs today often use proprietary record structures and have inter-operability problems. A secure communications link between the networks does *not* ensure that communications beyond that link are secure.

Some VPNs use a variety of non-IPSec protocols. These include PPTP, L2TP, L2F, and proprietary protocols. These protocols offer similar services but are better suited to remote-access applications and non-IP traffic across the public Internet. While these protocols have their uses, they are not covered in this document.

Principles

Principles in this document are fundamental truths a high conceptual level. The following Security Domain principles are ideas or concepts that frame and contribute to the understanding of technical topics and components noted above.

Principle 1. Ensure Security, Confidentiality and Privacy

IT systems should be implemented in adherence with all security, confidentiality and privacy policies and applicable statutes.

Implications

- Need to identify, publish, and keep the applicable policies current.
- Need to monitor and enforce compliance to policies.
- Must make the requirements for security, confidentiality and privacy clear to everyone.
- Education on issues of privacy and confidentiality must become a routine part of normal business processes.

Principle 2. Apply a level of security to resources commensurate to its value to the organization and sufficient to contain risk to an acceptable level.

Implications

- Security is a business enabler with associated costs. Security costs should be rationalized to the intended benefits.
- Requirements for security vary depending on the information system, connection to other systems, sensitivity of data, and probability of harm.
- Each transaction type will have individual security requirements.
- Security costs potentially increase beyond the value of the assets protected. Don't use more security than is required.

Principle 3. Resetting security assurance levels should not require modification of the architecture.

Implications

- Requirements for security vary depending on nature of communication, sensitivity of data, risks to the enterprise.
- Security services should be granular enough to accommodate assurance levels required.

Principle 4. Provide infrastructure security services to enable the enterprise to conduct business electronically.

Implications

- An architecture that defines an integrated set of security services permits state agencies to focus on the business goals rather than on the implementation of security.
- Integration of security services will enable interoperability and provide flexibility in conducting electronic business across and beyond the enterprise.
- Integration will reduce the costs of protecting the state's resources.

- Integration will increase the reliability of security solutions.
- Centralized Directory services

Principle 5. An accurate system date and time are essential to all security functions and accountability and must be maintained.

Implications

- The validity of digital signatures and electronic transactions depends on precise, reliable date and time information.
- Audit accountability relies on placing events sequentially according to date and time.

Principle 6. Perform a business-driven risk assessment for all automated systems.

Implications

- A risk assessment should be performed for all new and ongoing business systems. To determine the appropriate security requirements, business units should assess the value of system assets, risk exposure to those assets and evaluate the costs of protecting those systems.
- Understanding the value of assets and associated risks is essential to determining the level of security required.
- Security requirements should be included when designing or purchasing new applications.

Principle 7. Base application security on open standards where possible, industry standards when practical.

Implications

- Security services will be provided as infrastructure services. In order to take advantage of security services, application security must be designed for open standards. A clear migration path should be defined for products not yet capable of integrating with the infrastructure security services.
- Products from vendors are often implemented in ways that make it difficult to integrate these products into an overall security architecture.
- Clear identification of integration issues should be part of the design process. If necessary, a migration path should be defined.
  When selecting software requiring security, selection criteria must include:
  - Strict Adherence to open standards, such as OPSEC (Open Platform for Security), X.509v3 Certificates, SSL, S/MIME, LDAP, and SASL.
  - Avoiding platform-specific implementations that inhibit integration.

Principle 8. Use existing services consistent with open standards where possible, industry standards when practical.

Implications

- Security services exist for many common applications. Where possible, use existing services consistent with open or industry standards, such as OPSEC (Open Platform for Security).

- Web-enabled applications have Web browser to Web Server secure connections such as Secure Sockets Layer (SSL). Unless client authentication is required, basic SSL connections offer sufficient security to support many applications.
- Email clients can support secure messaging with S/MIME.

Principle 9. Locate security in the appropriate layer of a communications protocol to ensure maximum usability with minimum future modification.

Implications

- Whenever security is required, the location in a communications protocol will have an impact. The impact may be on performance, reliance on an underlying network protocol, and on developers. Choosing the appropriate layer in a communications protocol will maximize usability and minimize future changes.
- Security services can have an impact on performance. The impact is minimized when security services are located at lower layers of a communications protocol.
- Security services can have an impact on developers. For example, services provided at the transport layer have less impact on application programmers than services that run above that layer.
- Security services can increase reliance on a network protocol. An appropriate choice depends on the communication requirements of the business system.

Standards

Standards are listed and products are classified as “Obsolete”, “Transitional”, “Strategic”, or “Research”.

Obsolete Standards

It is highly likely that these standards or products, while still in use, will not be supported by the vendor (industry, manufacturer, etc.) in the future. Some products and standards have already reached the non-supported state. Plans should be developed by the agencies or the State to rapidly phase out and replace them with strategic standards or products. No development should be undertaken using these standards or products by either the agencies or the State.

Transitional Standards

These are standards or products in which an agency or the State has a substantial investment or deployment. These standards and products are currently supported by DOIT, the agencies, or the vendor (industry, manufacturer, etc.). However, agencies should undertake development using these standards or products only if there are no suitable alternatives that are categorized as strategic. Plans should be developed by the agencies or the State to move from transitional to strategic standards or products as soon as practical. In addition, the State should not use these standards or products for development.
Note: many older versions of *strategic* standards or products fall into this category, even if not specifically listed in a domain architecture document.

Strategic Standards

These are the standards and products selected by the state for development or acquisition, and for replacement of *obsolete* or *transitional* standards or products. (Strategic means a three to four year planning horizon.) When more than one similar strategic standard or product is specified for a technology category, there may be a preference for use in statewide or multi-agency development. These preferred standards and products are indicated where appropriate.
Note: some strategic products may be in “pilot testing” evaluation to determine implementation issues and guidelines. Pilot testing must be successfully completed prior to full deployment by the agencies or the State.

Research / Emerging Standards

This category represents proposed strategic standards and products that are in advanced stages of development and that should be evaluated by the State. The some of these standards or products may already be undergoing “hands-on” evaluation. Others will need to be tracked and evaluated over the next 6 to 18 months.

Component – Access Control

Firewalls

One of the most important requirements of a firewall is the ability to perform *Stateful Inspection*. *Stateful Inspection* provides the highest level of security possible by incorporating communication- and application-derived state and context information, which is stored and updated dynamically. This provides cumulative data against which subsequent communication attempts can be evaluated. *Stateful Inspection* provides full application-layer awareness without requiring a separate proxy for every service. This results in improved

performance, scalability and the ability to support new and custom applications quickly. These are just some of the reasons why *Stateful Inspection* has been adopted by customers as the firewall technology of choice.

Another important requirement is Ease of Use. The software must be straightforward and friendly, providing a helpful and intuitive interface.

Proxy

A proxy is server that sits between a client application, such as a Web Browser, and a real server. It intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server. Proxy servers can dramatically improve performance for groups of users. This is because it saves the results of all requests for a certain amount of time. Consider the case where both user X and user Y access the worldwide web through a proxy server. First user X requests a certain web page which we'll call Page 1. Sometime later, user Y requests the same page. Instead of forwarding the request to the Web server where Page 1 resides, which can be a time-consuming operation, the proxy server simply returns the Page 1 that it already fetched for user X. Since the proxy server is often on the same network as the user, this is a much faster operation. Real proxy servers support hundreds or thousands of users. Proxy servers can also be used to filter requests. For example, a company might use a proxy server to prevent its employees from accessing a specific set of web sites.

Component – Administration Tools

Intrusion Detection Systems

An Intrusion Detection System (IDS) is a collection of hardware and software components, which allows the real-time monitoring of network and computer events. These components can consist of network and host-based sensor programs, which constantly examine network and host traffic in order to compare network traffic and host log entries to the known and likely methods of attackers. Suspicious activities trigger administrator alarms and other configurable responses.

The result is comprehensive security assessment and management process, easily configured and administered from a central location.

Protocol Analysis

A protocol analyzer is a program and/or device that monitors data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information off a network. Unauthorized sniffers can be extremely dangerous to a network's security because they are virtually impossible to detect and can be inserted almost anywhere.

This makes them a favorite weapon in the hacker's arsenal. On TCP/IP networks, where they sniff packets they're often called *packet sniffers.* The state uses this component to troubleshoot complex network problems, and to collect raw traffic data when investigating and illegal or unauthorized network access.

Scanning and Penetration Testing

Scanning and penetration tools allow the security administrator to simulate a real attack upon networks and hosts. This capability provides a detailed vulnerability analysis of hosts,

routers, and assorted network components, which will assist in identifying and reducing security risks.

E-Mail Content Filtering and Virus Protection

This component is an important element in reducing the State's risk with E-Mail. Accidental or deliberate, confidentiality breaches are an increasing threat to organizations and can have a devastating effect on customer and market confidence. Replying to all recipients of a message, without checking the list for non-company employees, may lead to an unintentional leak of confidential plans.

On the other hand, the premeditated distribution of a customer database may be a calculated act of sabotage. Actions by disgruntled employees, information sent unintentionally, legal cases brought about by employees or "spam" and spoof attacks can all lead to adverse publicity for an organization. With the growth of Internet usage, the issue of legal liability manifested itself first in the USA, and consequently across the rest of the world. Cases involving e-mail misuse and sexual or racial harassment via e-mail have resulted in legal liability lawsuits with multi-million dollar penalties.

Traditionally, employers have been responsible and liable for the actions of their employees in the workplace. However, if an organization can demonstrate a 'duty of care' to reduce unacceptable employee activity, then it could minimize its potential for liability. It's all too easy for employees to utilize e-mail and the Web during work hours, for non-work related activities. In a recent study by the American Management Association, 64% of employees have access to e-mail and 48% to the web. In March 1999 the CSI/FBI Computer Crime and Security Survey reported that 97% of responding organizations had experienced employee abuse of the Internet. They estimated that the cost in lost productivity incurred by an employer with 1,000 employees could be as much as $96,000 per year. The circulation via e-mail amongst employees of nude and pornographic images is more commonplace than one might think.

Theft of Data - this can take many forms. For example, an employee could send confidential data out of the organization either maliciously, or unintentionally, perhaps by replying to a spoofed e-mail.

Spoofing - this refers to an e-mail where the identity of the sender is disguised to look like it's come from a reputable source. This can have disastrous consequences in terms of loss of trade secrets, betrayal of client confidentiality or theft of data. Data can be corrupted in many ways but the most common occurrence is through e-mail virus attacks, which today account for at least 95% of all attacks reaching the desktop (Ferris Research, 1999). Other causes of data corruption include worms, Trojans, malicious mobile code and hoaxes.

GAP ITEM Content Technologies MIMESWEEPER

Centralized LAN/WAN Management Console

In order to maintain specific uptime requirements of a large enterprise network, a centralized LAN/WAN Management Console is needed. This hardware/software component provides:

- Asset Management to automate the processes that track the state's assets,
- Availability Management, which supports business applications and computing resources to maximize their availability for improving customer service levels,

- Change Management, which helps manage the necessary changes to a dynamic computing environment,
- Network management, which assists in keeping network devices up and running, and
- Operations Management, which centralizes control of all back office operations.

Component – Identification/Authentication

Mainframe

ACF2, RACF, MAPPER

Remote Access

Nortel Contivity VPN

Authentication Servers

RADIUS

Strong Token

SecureID

Biometrics

Research needs to be undertaken Thumb Scanners, Face Geometry, ETC

Component – Cryptography

Public Key/Private Key

Currently, there is no PKI standard in use in the state of Connecticut.

Digital Signatures

Currently, there is no Digital Signature standard in use in the state of Connecticut.

Secret Key Technology

Secret key technology is being used in rare circumstances where remote access is required to security infrastructure components such as firewalls, intrusion detection systems and distributed protocol analyzers. As a minimum, 3-DES is required for such communications. However, no standard has been implemented across the enterprise.

Security Protocols

Security protocols such as SSLv3, SKIP, MIME, S/MIME, IPSec, IKE and ISAKMP are available for use, but are not incorporated across the State enterprise as a standard.

Virtual Private Networks (VPN)

Currently, the state is using a VPN for secure remote communications. With the prospect of mandated encryption for Healthcare systems in the near future, a strong case can be made for the expansion of the existing extranet VPN for this Purpose.

Table 1 Security Domain Product Standards 1

Security Domain Standards

Entries in Italics are suggestions for items missing or not yet identified.

COMPONENT	Obsolete	Transitional	Strategic	Research
Firewall				
Cisco PIX		✓		
BorderManager		✓		
Checkpoint			✓	
Proxy				
WebTrack SMARTFILTER			✓	
N2H2				✓
Admin Tools				
Intrusion				
ISS RealSecure			✓	
Protocol Analysis				
NAI Sniffer Pro			✓	
Scanning/Penetration				
IIS Internet Scanner			✓	
L0phtCrack			✓	
Lan/Wan Management				
Landesk	✓			
Managewise	✓			
ZenWorks	✓			
Tivoli			✓	
CA-Unicenter TNG				✓
Virus/Content Filtering				
Content Technologies MimeSweeper				✓
TrendMicro				✓

Entries in Italics are suggestions for items missing or not yet identified.

Table 2 Security Domain Product Standards 2

Security Domain Standards

Entries in Italics are suggestions for items missing or not yet identified.

COMPONENT	Obsolete	Transitional	Strategic	Research
Directory/Authentication				
Mainframe				
ACF2			✓	
Mapper(Unisys)			✓	
RACF				✓
Remote Access				
Nortel VPN			✓	
Checkpoint VPN-1				✓
RNAS		✓		
Authentication Servers				
Radius			✓	
Strong Token-based				
SecureID			✓	
ACE			✓	
Directory				
NDS			✓	
LDAP				✓
Physical/Biometric				
Thumb Scanners				✓
Visual Face Recognition				✓
Cryptography				
Secret Key			✓	
Public Key/Private Key				✓
Digital Signatures				✓
Securtiy Protocols				
SSLv3			✓	
IPSec			✓	
VPN			✓	
Nortel Networks Contivity Switch			✓	
Checkpoint VPN-1				✓
Best Practice				
Enterprise Security Policy			✓	
Enterprise Change Control Policy			✓	
Network Security Engineering Standards			✓	

Best Practices

Given that the State of Connecticut Enterprise network is composed of many independent, separately managed and differently designed systems, the establishment of a single cohesive and global security domain definition is extremely difficult. Based upon existing implemented strategic initiatives, the following best practices are designed to maximize effective promulgation of those initiatives.

Best Practice #1 – Security Policy

Identify Security Policy Domains

These could be defined along agency or organizational lines. Establishing security domains simplifies the analysis of security requirements and focuses attention on security policy requirements. For example, in addition to the State's Enterprise Security policy, which may be considered the overall or umbrella document, an agency or government branch may have a specialized set of policy components. These components are specifically pertinent to its operation (e.g., State Police, Judicial Branch, and Legislative Branch). Please see the State of Connecticut Enterprise Security Policy located in the Appendix. This policy was created by DOIT to address security rules and issues affecting the enterprise network.

Within each Policy Domain

Identify and publish the security policy, and maintain the currency of such policies. Governance must be granted to monitor and enforce compliance to policies in order to ensure security, confidentiality and privacy based upon existing laws and applicable statutes.

Establish a working group across the enterprise consisting of all Enterprise Network user agencies and business partners. This will provide education on the issues of security, privacy and confidentiality; this education must become a routine part of normal business processes.

Best Practice #2 – Implementation of Security Architecture

Because security control impacts the entire enterprise, its implementation must be easy to administer, verify and sustain. Care should be taken to adhere to industry proven or open standards when designing the architecture. Centralized control is a crucial element in making the architecture easy to administer. For example, when deploying firewall technology across the enterprise, a single, centrally managed product should be chosen, not a collection of multiple disparate systems, which are not compatible.

Best Practice #3 – Provide the Capability to Monitor All Relevant Activity

To establish accountability, a capability to track and monitor all relevant activity must be made available. In order to detect security violations, and to test if the security infrastructure components are behaving as designed, products and services must be deployed to assist the security administrator.

Appendix – Network Security Policy

Network Security Policy and Procedures for use by all State Agencies

Version: 1.0 **Date Issued**: April 2, 1999 **Date Effective**: April 29, 1999

Purpose

The Department of Information Technology (DOIT) for the State of Connecticut, under the authority granted to the Chief Information Officer in Sec. 4d2. of the Connecticut General Statutes, has established this policy and reporting requirements, and associated standards to assure that critical information is protected and data flow is not interrupted by unauthorized access.

Policy Statements

The following policy statements are abstracted from the official State of Connecticut Network Security Policy.

1. All information travelling Over State computer networks that has not been specifically identified as the property of other parties will be treated as though it is a State asset. If there is no primary agency designated to administer this information, DOIT will become the steward of this data until another agency is designated. It is the policy of the State to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information.
2. In addition, it is the policy of the State to protect information belonging to third parties--that has been entrusted to the State in confidence--in the same manner as private sector trade secrets as well as in accordance with applicable contracts.
3. All computers permanently or intermittently connected to State of Connecticut networks, and all DOIT computers that intermittently or continuously connect to an internal or external network must employ password-based access controls. must have password access controls. All users must be positively identified prior to being able to use any multi-user computer or communications system resources.
4. The computer and communications system privileges of all users, systems, and independently operating programs (such as "agents") must be restricted based on the need-to-know.
5. Participation in external networks as a provider of services that external parties rely on is expressly prohibited unless the Agency System Administrator has identified, in writing, the security risk involved and submitted them to the Security Review Committee, and the Chief Information Officer has expressly accept these and other risks associated with the proposal.
6. Any modification in existing Network/Systems configurations, that is in contrast to the Statewide Security policy must be submitted for approval to the Security Review Committee.
7. Each agency that has existing dial-up lines/modems today must submit a request for consideration of approval to the Security Review Committee.
8. Wireless communications, or other broadcast technologies, must not be used for data transmission containing State "confidential" or "restricted" information unless the connection is encrypted and has an acceptable level user authentication.
9. Third party vendors must NOT be given dial-up privileges to State computers and/or

networks unless the involved system administrator determines that they have a bone fide need. These privileges must be enabled only for the time period required to accomplish the approved tasks (such as remote maintenance).

10. All users wishing to use the State internal networks, or multi-user systems that are connected to the State internal networks, must sign a *compliance statement* prior to being issued a user-ID.
11. State workers in the possession of portable, laptop, notebook, palmtop, and other transportable computers containing "restricted" or "confidential" State information must not leave these computers unattended at any time unless the information is stored in encrypted form. Transportable computers containing unencrypted "restricted" or "confidential" information must remain in the possession of the State worker traveler when traveling.

Implementation of the Policy

An Implementation Committee, composed of DOIT and other agency IT staff, will assist agencies in gaining initial compliance with this policy. The Implementation Committee will review the following actions by agencies:

Designate a information security liaison.

Each agency must determine what agency information is confidential or restricted, and submit this information in writing

Each agency that has existing dial-up lines/modems today must submit a request for review and approval.

An Agency that has it's own Internet connection today, must submit the following information:

1. Name of the Internet Provider and line speed of the circuit.
2. Model and type of Firewall hardware and software.
3. Port numbers that are opened in the Firewall.

The Security Review Committee will initially review:

1. Agency developed security policies.
2. Any modification in existing Network/Systems configurations that may not conform to the Statewide Security policy.

Agency Planning and Reporting Responsibilities

Planning:

4. Each State agency will develop it's own network security policy. The agency security policy will address:

a. System Access Control which includes how to choose passwords, how to set-up passwords and log-in/log-off procedures,
b. System Privileges; limiting system access, process for granting system privileges and the process for revoking system privileges and Establishment of Access Paths;
c. Computer Network Changes; conditions for participation in external networks, policy for initiating session via dial-up lines, establishing wireless communications and discussion of computer viruses, worms, and Trojan horses.

3. Each agency, must determine what agency information is confidential or restricted
4. The agency network security policy will be incorporated in the agency's Information

Technology plan and architecture document.

Reporting:

5. As of July 1, 1999, each agency will submit the information required in **[**Attachment A**]** of the official policy statement to to Jim McGill, Enterprise Network Manager.
6. Any modification in existing Network/Systems configurations, that is in contrast to the Statewide Security policy must be submitted for approval to the Security Review Committee

Any agency that has it's own Internet connection today or will have in the future, must submit the following information to the Security Review Committee:

a) Name of the Internet Provider and line speed of the circuit
b) Model and type of Firewall hardware and software.
c) c) Port numbers that are opened in the Firewall.

Compliance:

5. Each agency must submit it's own Network Security Policy to the Security Review Committee for review and approval.
7. Each State Agency must have a designated information security liaison. The name, telephone number and email address of the individual or individuals must be sent to Jim McGill. email address: james.mcgill@po.state.ct.us This information must come from the Commissioner or IT Manager level.

Any modification in existing Network/Systems configurations, that is in contrast to the Statewide Security policy must be submitted for approval to the Security Review Committee.

Scope

This policy applies to the following entities: any State of Connecticut agency, institution, office, department, commission, council or instrumentality that utilizes State owned and maintained data networks in the conduct of its business.

Definitions

State Agency: For the purposes of this policy, the term *State Agency* refers to any State of Connecticut agency, institution, office, department, commission, council or instrumentality.

C*ompliant:* For the purposes of this policy, an agencies network security policy considered compliant when it meets the criteria defined in, and/or performs as described in, the State Network Security Policy.